REMARKS

Claims 1-3 were rejected under 35 U.S.C. §102(b) as being anticipated by Holloway et al. (US 5,805,801) in view of Sofer et al. (US 5,489,896). The applicant respectfully traverses this rejection for the following reason(s).

We will assume the rejection is under §103(a) and rejects all claims.

Claim 1

Claim 1 calls for, in part, *detecting, in an address table, access vectors corresponding to the MAC destination and source addresses.*

The combination of applied art fails to teach the foregoing feature.

Holloway's invention relates to systems and methods for detecting and preventing intrusion into a campus local area network by an unauthorized user. A managed hub discovers each interconnect device in the network that supports the security feature and maintains an interconnect device list of such devices, which may include token ring switches, Ethernet switches, bridges and routers. The managed hub determines the interconnect devices in the campus network that are capable of supporting a local area network (LAN) security feature. The managed hub then uses the responses to build and maintain a table of interconnect devices in the network that support the security feature. Here, during a discovery phase, the managed hub periodically sends a discovery frame to a LAN security feature group address. The managed hub detects an intrusion by an unauthorized address on one of its ports by comparing the MAC addresses on each port against a list

of authorized MAC addresses, disables the port and notifies the other interconnect devices in the network of the intrusion by transmitting a security breach detected frame to the LAN security feature group address. The interconnect devices set a filter on their respective ports against the intruding unauthorized address.

Sofer's invention relates to a security unit for a network having a data bus to which a plurality of stations (interconnect devices) can be connected wherein the security unit monitors traffic on the data bus and only enables authorized data to flow along the data bus. The data bus and the security unit are part of a hub. The traffic includes a multiplicity of data packets each having source and destination addresses and the security unit includes a plurality of correlators for determining that the source and destination addresses indicate an authorized communication. Additionally, each station is connected to the data bus via a port having a port address and one of the correlators correlates the source address with an authorized port address.

Note that Sofer's port address is not the same nor equivalent to a destination address, as Sofer clearly differentiates the two addresses. A destination address is the final destination for the message, where the port address is for a particular port connected to the final destination.

Sofer differs from Holloway in that Sofer teaches the destination station address be in a list of authorized destination station addresses for the source station address, because Sofer is concerned with permitting two stations being authorized to communicate with each other. Holloway is only concerned with intrusion by an unauthorized source station outside the network breaking into the network via one of the ports. There is no concern with whether a source station is authorized to connect to a destination station.

If one of ordinary skill in the art were motivated to modify the security of a network utilizing Holloway's system in the manner taught by Sofer, then the skilled artisan would modify the system as taught by Sofer.

Here, Sofer discloses an authorization unit 44 that comprises three correlators 50, 52 and 54, a mode switch 56 and a decision unit 58. Correlator 50 determines whether or not the source station address is among authorized source stations. Correlator 52 determines whether or not the source station address is attached to its corresponding port, where the port address is provided from a hub 20, in the case of the LET 36 hub. Correlator 54 determines whether or not the source station is allowed to communicate with the destination station. Each of correlators 50-54 comprise a list of authorized relationships. Thus, correlator 50 has a list of authorized stations, correlator 52 has a list of source addresses and their corresponding port addresses and correlator 54 has a list of source addresses and their allowed destination addresses.

As mentioned above, claim 1 calls for *detecting, in an address table, access vectors corresponding to the MAC destination and source addresses.*

None of Sofer's correlators utilize access vectors, but instead use specific addresses, and similarly Holloway discloses the use of an authorized address list (AAL) controls which MAC addresses are allowed to connect to <u>specified ports</u>. Each entry in the AAL consists of two fields: port number and authorized address. The port number identifies a specific port on the hub; the authorized address field specifies the address or addresses that are allowed to connect to the port. The AAL (Authorized Address List) defines which MAC source addresses, *i.e.,* authorized source address, are allowed to connect to specific ports on the hub.

Accordingly, neither of the applied references would have taught one of ordinary skill in the art to utilize *access vectors*, which are not equivalent to access addresses, instead of MAC addresses.

The present invention has an advantage over the applied art, because of its use of access vectors. An access vector consists of a bit vector. The bit value "0" means restriction to access and "1" means allowance for access. For example, if a server node S1 has an access vector 00010000 and a client node C1 has access vector 10000001, then client node (source station) C1 cannot access server node (destination station) S1, but another client node C2 having access vector 00010001 can access server node S1.

For further understanding, access vector 00010000 of a server node S1 means that S1's HostID is 3, and its access vector is 0x80>>3. If C1 is going to be an access client node, the access vector of C1 should be (0x80>>3). If the access vector of C1 is 10010001, then this access vector 10010001 means C1 can access server nodes that have HostID 0, 3 or 7. Thus a client node having an access vector xxx1xxxx (x can be a 0 or 1) can access a server node having a HostID of 3, and a client node having an access vector xxx0xxxx (x can be a 0 or 1) is restricted from accessing a server node having a HostID of 3.

Accordingly, it is possible to use the same (e.g., 8-bit) access vectors for more than one (32-bit) source address and (32-bit) destination address, thereby saving memory space for storing the correlating 8-bit access vectors instead of correlating each 32-bit source address and destination address.

Therefore, since the present invention utilizes access vectors instead of the MAC addresses of the prior art, and the applied art fails to teach or move one of ordinary skill in the art to use
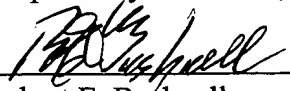
anything other than MAC addresses for preventing or allowing access, the rejection of claim 1 is deemed to be in error and should be withdrawn.

Claims 22-28 are deemed to be patentable over the art of record for the same reasons as claim 1.

The Examiner is respectfully requested to reconsider the application, withdraw the objections and/or rejections and pass the application to issue in view of the above amendments and/or remarks.

Fees for filing an RCE and a Petition for an extension of time accompany this Amendment. No fee is incurred by the amendments to the claims set forth in this Amendment. Applicant's check drawn to the order of Commissioner accompanies this Amendment. Should the check become lost, be deficient in payment, or should other fees be incurred, the Commissioner is authorized to charge Deposit Account No. 02-4943 of Applicant's undersigned attorney in the amount of such fees.

Respectfully submitted,

Robert E. Bushnell
Attorney for Applicant
Reg. No.: 27,774

1522 K Street, N.W.
Washington, D.C. 20005
(202) 408-9040

Folio: P56339
Date: 3/29/06
I.D.: REB/MDP

-11-